The Need to Address Mobile Device Security in the Higher Education IT Curriculum

Karen P. Patten
Mark A. Harris
Integrated Information Technology
University of South Carolina
Columbia SC 29053 USA
pattenk@hrsm.sc.edu maharris@hrsm.sc.edu

ABSTRACT

Mobile devices, including smartphones and tablets, enable users to access corporate data from anywhere. In 2013, people will purchase 1.2 billion mobile devices, surpassing personal computers as the most common method for accessing the Internet. However, security of these mobile devices is a major concern for organizations. The two leading mobile operating systems (OS), Google's Android OS and Apple's iOS, both have security concerns as do the mobile applications and the major application markets. 'Bring your own devices,' where employees supply their own equipment for work-related purposes, can cut costs for organizations, but failing to address security can significantly increase those costs. This paper focuses on the increasing need for mobile business and its related mobile device security concerns. We propose that future IT professionals should be aware of these issues and learn how to secure mobile devices through the integration of the topic into the IT Model Curriculum. Using the case of one undergraduate IT program, we developed a set of mobile device security education recommendations, which we then mapped to the IT Model Curriculum using the guidelines from Accreditation Board for Engineering and Technology (ABET). This mapping approach demonstrates one way how higher education institutions could integrate mobile device security into any IT curriculum.

Keywords : Mobile computing, Information assurance and security (IAS), ABET, Model curricula, Curriculum design and development

1. INTRODUCTION

As of January 2013 in the United States, Android made up 52.69 percent of mobile device operating systems and Apple iOS accounted for 34.9 percent (Statcounter, 2013). Apple iOS had the lead only eighteen months earlier. Since the summer of 2011, Android has steadily taken over the market from iOS as the most popular mobile operating system with all other platforms, like Windows Mobile, Symbian, and BlackBerry, accounting for less than thirteen percent combined (Statcounter, 2013).

Mobile devices include smartphones and tablets, both of which have become very popular among consumers. In 2013, people will purchase 1.2 billion mobile devices, surpassing PC's as the most common method for accessing the Internet (Lookout, 2013). Many of these devices will not only be used for personal activities, but for work-related activities as well. Bring Your Own Device (BYOD) has become very popular and leads to many security concerns for information technology (IT) security professionals. The SANS Institute recently reported 61 percent of respondent's organizations allowed BYOD access to resources (SANS, 2012). That percentage is expected to rise as the number of devices increases, the functionality of the devices becomes that of a PC, and work becomes mixed with play beyond the traditional 9-5 Monday through Friday work week. *"For many organizations today, the BYOD issue is less a matter of 'No, we can't do it' and more a question of 'how do we do it'* (Thomson, 2012)?"

Mobile devices, including BYOD and corporate issued devices, all pose new problems for IT professionals who do not quite know how to handle the problem yet. A recent study of IT security professionals revealed 68 percent of them have no way of identifying known mobile device vulnerabilities on their networks (Tenable-Security, 2012). *"Nearly all survey respondents said mobile devices present a security threat to their business, yet 67 percent said they either have no controls in place for mobile device usage on their network or employees simply ignore existing mobile device usage policies* (Tenable-Security, 2012)." A primary reason this technology is causing so many concerns is that it is new and rapidly evolving.

Employees do not understand the threats to mobile devices as they do their desktop PCs. IT security professionals do not fully understand the implications this technology has on the company and the steps needed to protect corporate assets. One solution is education. Everyone needs to be educated on mobile device security

and the best place to start is with college students, especially those in information technology programs. Those already in the workplace will have to play catch up, but a good start is to educate those entering the workforce.

This paper reviews mobile device security concerns and develops recommendations for education that are in line with Accreditation Board for Engineering and Technology (ABET) accreditation standards. An example is given of how those recommendations are being adapted at a university currently applying for ABET accreditation. The following sections provides a literature review of the business needs for information security and mobile device security (MDS), the emerging mobile device technical issues, and the evolution of the IT curriculum including the need for information assurance security (IAS) and MDS within the IT curriculum. This paper then suggests mobile device security education recommendations, which are mapped to the Model IT Curriculum as an approach for integrating the MDS into any undergraduate IT program.

2. BUSINESS NEED FOR MOBILE DEVICE SECURITY

Information security issues within enterprises are becoming more complex daily. However, with increased global business demands, enterprises are finding new areas of security concerns. Annually, since 1980, the Society for Information management (SIM), together with leading academic researchers, surveys IT executives about their management concerns as well as application and technology investments and organizational considerations. The top ten management concerns are tracked from year-to-year. Security and privacy, one of the 'traditional' concerns, continues to be one of the top ten concerns year after year. Although it ranked as high as third in the early 2000s, security and privacy has dropped to ninth in the latest 2011 results, primarily due to problems from the current economic pressures on global businesses. Security and privacy maintains its top ten ranking due to the need for enterprises to protect valuable information assets such as trade secrets, new product development, and customer data. In this same survey, however, security ranked 32nd out of 51 important technologies. Luftman and Derksen (2012) attribute this to the attitude that security is considered to be more of a management issue than a technical one. Doomun (2008) suggests that security be considered from three different perspectives: technological, risk, and compliance. The information security architecture within an organization is affected by its information security policy, its risk management, and its internal control and auditing processes. Risk management is essential to identify the assets and threats to information security. Internal controls to refer to technical controls based on standards and governance.

Although employees are working remotely, their need to be 'connected' to corporate offices is rapidly increasing. Mobile employees, in one study over a five year period, initially used mobile devices as communications devices to stay in touch with others and to work remotely. But, over time, the same employees shifted their use to the need to have instant access to corporate data because of the increased need to be more productive and perform in dynamic environments (Dery and MacCormick, 2012). Because employees could not access many services and applications on company-provided Blackberrys, employees started using their own personal mobile devices. They were using mobile technologies such as smartphones and tablets to interact with their customers, vendors, and colleagues from anywhere at any time.

Business mobility trends will continue as more employees purchase and use their personal smartphones and tablets for work-related activities, which will require a growing number of enterprises to support bring-your-own-device (BYOD) programs (Forrester, 2012). The shifting needs of employees from being able to communicate to being always connected further increases the complexity of securing an enterprise's information resources. The 2011 SIM survey (Luftman and Derksen, 2012) identified the 'top ten applications and technology developments for 2003-2012.' Mobile and wireless applications, currently listed sixth, have been on the top ten list for the last four years. For the first time in 2011, BYOD mobile devices also entered the top ten list as seventh. Forrester Consulting (2012) reported that the top priority for 64 percent of the responding firms in Europe and North America was providing more mobility support for employees. The following section describes the types of mobile device security issues that are impacting today's businesses.

3. MOBILE DEVICE SECURITY CONCERNS

The popularity of smartphones and tablets poses new threats and issues for the enterprise. This section describes many of these new threats from mobile devices.

3.1 Malware

Malware is a rapidly growing problem for mobile devices as forecasts predict that people will download seventy billion apps in 2014 (Lookout, 2013). During the calendar year of 2012, Lookout (2013) estimates eighteen million people will encounter Android malware. Android malware is on the rise at much higher rates than is Apple iOS. TrendMicro (2012) reported an increase from one thousand Android malware samples in 2011 to 350,000 in 2012. The number of high-risk malicious malware apps for Android in just three years is significant compared to the fourteen years it took the PC to reach those numbers (TrendMicro, 2012). Android now exceeds PCs for malware attacks in the United States (Mansfield-Devine, 2013). Just over 99 percent of all malware detected in 2012 was written for Android, with less than one percent from the other operating systems (Kaspersky, 2013).

The most popular category of malware for all platforms was SMS premium text messaging malware. This type of malware can send premium pay text messages without the user's knowledge. Just over 78 percent of Lookout's 2012 malware detections fall into this category and cost the average user $9.99 a month (Lookout, 2012). TrendMicro and ESET Security also reported that SMS premium text messaging was the top malware variant (ESET, 2013; TrendMicro, 2012).

Fake applications are another major malware problem, and both Android and Apple are affected. Fake applications

look and work like the real thing, but contain malware code as well. Security firm Arxan reports that 100 percent of the top 100 apps for Android and 92 percent of the top 100 apps for iOS have fake malware versions available as of mid-2012 (Arxan, 2012). Most fake malware applications are most commonly found on third party application sites, which are easy to access for Android and difficult for iOS.

3.2 Android

Android is an open source platform, meaning the underlining programming code is made public, but with some restrictions. This allows device manufactures, carriers, and others to modify the software, which gives them more flexibility in creating cutting-edge applications. The openness of the platform and the tools made available from Google encourage developers to write applications and also leads to quicker development.

Applications developed from Android can be quickly submitted and made available on the Google Play market or through third party markets. A problem with the Google Play market is the lax vetting process of software developers and software applications, which are nowhere near as extensive as Apple's vetting process (Greenberg, 2012). Even worse is the vetting process for the third party markets, where much of the Android malware is found (Arxan, 2012). However, not all Android third party markets are the same, which leads to confusion. Some have similar vetting processes to Apple, such as the Amazon's Appstore for Android (Strohmeyer, 2011).

Google has recently attempted to address the problems with the Google Play market malware apps by scanning new applications for known malware and testing new applications in a simulated environment (Greenberg, 2012). However, this does not account for software applications downloaded from third party markets. To fix this, the latest version of Android as of early 2013, Jelly Bean 4.2, has built-in malware scanning to check apps for harmful behavior when first installed. This version also added a feature that would alert the user anytime an app attempts to send a text message that could cost the user money (Raphael, 2012). However, the new app scanner does not address the issue of apps changing their behavior after installation (Unknown, 2012). This is a problem where apps execute new code after installation, which bypasses the application screening process (Greenberg, 2012).

Part of the problem with the Android platform is the availability of multiple carriers and vendors that do not follow a particular standard, leading to old versions of the OS still on the market (Mansfield-Devine, 2012a). As of January 2013, only 1.2 percent of the devices on the market had the latest version (Platform Versions, 2013). The previous version only accounted for nine percent of the market. The two most popular versions on the market are 2011's Ice Cream Sandwich (29.1 percent) and 2010's Gingerbread (47.6 percent).

Adding to the problem of older versions of software in the market are delays in updating or patching operating system software. Research suggests that the time it takes for half of the Android users to update their software was eight to ten months and the likelihood they would buy a new device was greater than the likelihood they would update their old device's software (Mansfield-Devine, 2012a).

3.3 Apple iOS

Contrary to how the Android platform works is the Apple iOS platform. The apple operating system is not open and is controlled by Apple. Only one manufacturer makes devices for the platform and there is no fragmentation of the operating system (Mansfield-Devine, 2012c). In contrast to Android's fragmented OS with many versions still on the market, Apple claimed that over eighty percent of iPhone and iPad users had the latest iOS as of June 2012 (Mansfield-Devine, 2012a).

Other security benefits from Apple are that users are forced to download apps from the Apple's App Store and there are no allowable third party markets. Users must jailbreak their devices to access third party markets and that is not permitted by Apple. Jailbreaking is discussed later.

Software updating is another advantage for Apple iOS. By default, the latest version of iOS as of early 2013, version 6.1, uses Apple's App Store to check for updates and patches. The older iOS version 5 uses Over-the-Air (OTA) to update (Mansfield-Devine, 2012a). Both methods are easy for users and patching software is highly encouraged by Apple, leading to more up-to-date and patched devices.

Overall, Apple iOS is more secure for the opposite reasons Android is less secure. Where Android has an open platform and encourages software app development and quickness to the market, Apple has a closed platform and the thorough vetting process discourages application development by many, slowing the time-to-market. The open nature of Android allows third party markets to exist and users to install third party apps with ease. The closed nature of Apple iOS prevents the use of third party markets for apps, thus forcing some users to jailbreak their Apple devices from the restrictions.

3.4 Jailbreaking and Rooting

Jailbreaking is a term mostly used with Apple devices. Jailbreaking a device removes the platforms restrictions, allowing users to install any application from anywhere, install a modified operating system, and have super-user root permissions. Rooting is often referred to as a similar process performed on Android devices. Rooting a device is typically done to give the user super-user root permissions, which allows them to overcome limitations placed on the device by carriers and device manufactures. Apple users often jailbreak their devices to access third party market applications and to fully customize their devices. Android users often root their devices to remove extra software installed by vendors and to install newer versions of Android, which are not supported by vendors.

A large percentage of Apple iOS devices are jailbroken because many people that like Apple products, do not like being limited (Mansfield-Devine, 2012c). For example, the new version of Apple iOS 6.1, released in January 2013, had seven million jailbreak downloads in the first four days on the market (Greenberg, 2013).

The security concerns for corporations are understandably high. Jailbroken and rooted devices pose tremendous threats to any organization because much of the

security that protected the devices has been removed. Because of such concerns, many IT security professionals have called for a ban of all jailbroken and rooted devices on corporate networks (ZDNet, 2013).

3.5 Android Permissions

Permissions are rights that an application has to access certain data and functionality on a device. For example, the permission for 'network communication' gives an application full Internet access. Applications state what permissions they want upon installation and the user has to agree to them in order to install the app. The user cannot selectively choose permissions. They must accept them all or not install the app. However, there are multiple problems with this permission based model used by Android. One is that users do not fully understand what the permissions actually mean and another is that many apps ask for more permissions than they really need (Hoffman, 2013).

Juniper Networks analyzed 1.7 million apps on the Google Play Android market and discovered a significant number of apps had permissions to obtain sensitive user data that the app may not need and many also had Internet access that could potentially transmit such sensitive data (Hoffman, 2013). In addition, Juniper found that free apps where much more likely to access personal information than were paid apps. Specifically, free apps are 401 percent more likely to track a user's location and 314 percent more likely to access the user's address book than were paid apps (Hoffman, 2013). Free apps were 2.5 times more likely to have permission to access the device's camera. Free apps were also nearly twice as likely to have permission to silently send text messages and over three times as likely to have permissions to clandestinely initiate calls in the background (Hoffman, 2013). This problem is going to get worse before it gets better, as Gartner predicts the number of mobile apps downloaded in 2013 will double to 45 billion with free apps accounting for nearly ninety percent of them (Gartner, 2013).

3.6 Android App Development

Many of the problems with Android do not come from malicious activity in the form of traditional malware, but from poor programming practices (Mansfield-Devine, 2012b). Many applications on the Android market provide poor security which is due to poor understanding of the security protocols (Fahl et al., 2012). This may be because of the ease of submitting applications to the Android markets. *"You don't need much in the way of resources in order to develop and market an Android app,"* and *"you also don't need much in the way of experience or knowledge* (Mansfield-Devine, 2012b)." For example, during development, apps are set to be debuggable, but developers sometimes forget to turn this off before releasing the application (Mansfield-Devine, 2012a). This allows a malicious app to pose as a debugger and get an app to do things it should not.

The availability of fake applications can be traced back to software development, which may have correctly followed typical approaches. However, traditional approaches to app security do not protect against new attack methods (Arxan, 2012). Arxan estimates that 95 percent of popular apps do not contain proper security to adequately prevent hacking, thus resulting in reverse-engineered fake malware versions of popular apps for all platforms (Arxan, 2012). Arxan states that properly secured apps do not have flaws or vulnerabilities, are protected against hacking, and maintain and self-defend their integrity (Arxan, 2012). This can be accomplished by assessing risks and attack targets in the app, hardening the code against reverse-engineering, and making the app tamper-proof and self-defending (Arxan, 2012).

4. MOBILE DEVICE SECURITY BUSINESS PRACTICES

Organizations that allow the use of mobile devices should, at a minimum, develop a mobile device policy, and, at best, implement mobile device management business tools.

4.1 Mobile Device Policy

If an organization allows mobile devices in the workplace, whether BYOD or corporate-issued, management should consider security policies. However, many organizations have not made such considerations. A McAfee survey found that 71 percent of organizations that allow professionals to use their own devices for work purposes have no policies in place to ensure data protection (McAfee, 2012). A SANS Institute survey found that only 41 percent of respondents feel strongly that they have policies to support BYOD (SANS, 2012). Results also indicated that 56 percent of respondents either did not have a policy regarding mobile devices or 'Sort of' policies (SANS, 2012). Much of the problem with developing policies and managing mobile devices in the enterprise is due to the complex nature of the devices and security management needed to protect them.

4.2 Mobile Device Management (MDM)

Mobile Device Management (MDM) is software or hardware that is used to manage and secure mobile devices in the workplace. MDM systems can be used to secure all of the popular platforms and models of mobile devices at the same time within the same system. So no matter what device and operating system is on the network, a MDM solution can configure and secure it. Security policies can be enforced, such as preventing jailbroken or rooted devices from accessing the network.

Another feature that can be integrated with a MDM solution is Mobile Application Management (MAM). Where MDM manages the physical devices, MAM services manage mobile applications, including development and deployment. Minimum MAM features include application whitelists and blacklists, enterprise application stores, application security, and data wipe by application (Rubens, 2012). Organizations can host their own application markets that users must use to access mobile device apps. If a user wants a specific app available on Google Play, Apple's App Store, or other markets, they request approval from their enterprise IT organization. IT can test the app before placing it on the corporate app market, making it available to corporate users.

5. EVOLUTION OF THE IT CURRICULUM

As early as the late 1990s, educators were beginning to recognize the need for the development of a separate IT

computing discipline. The economy experienced a tremendous growth in the need for professionals trained in information and communications technologies. Enterprises were beginning to realize that their global business success required more and more reliance on information and computing technologies. New and emerging technological advances, including wireless, graphical user interface (GUI), Internet, Web-development, new applications, all required resources to develop and manage them. More and more individuals were using information and computing technologies to do their work, but were not trained nor had expertise in information and computing technologies (Ekstrom et al., 2006).

Employers demanded new skills not part of computer engineering and computer sciences. Information Systems (IS) partly filled the gap because IS students had a better understanding of organizations and how IT applications support the organizations. However, these students did not have enough technology skills. Also, business schools were limited on how many courses could be offered in IS or management information systems (MIS) programs. Therefore, universities introduced fledgling undergraduate IT programs, although less homogeneous than other computing disciplines, there still was a core 'family resemblance.' Most of these early IT programs included networking, Web development, and system administration. Many of these early programs evolved from existing computer science, computer engineering, computer engineering technology, or information systems (Ekstrom et al., 2006). They existed in colleges of computing, computer science departments, schools of technology, and business schools. Early IT professors possessed degrees in IS, electronics, communications, graphics arts, economics, mathematics, and computer science. One of the authors of this paper was a full-time MIS instructor in a school of management with a joint appointment in the evolving IT program within the college of computing sciences in the early 2000s. Two different interpretations of IT evolved from these early programs: (1) *"Information Technology (IT) in its 'broadest sense' encompasses all aspects of computing technologies focused on meeting the needs of users within an organizational and societal context"* (Lawson et al., 2005); or (2) *"IT, as an 'academic discipline,' focuses on meeting the needs of users through the selection, creation, application, integration, and administration of computing technologies"* (Ekstrom et al., 2006, p. 348).

5.1 The IT Model Curriculum

In December, 2001, the evolution of the IT Model Curriculum began with the first Conference on Information Technology Curriculum (CITC-1) where participants used a Delphi study to identify curricular topics for an IT curriculum. The Society for Information Technology Education (SITE) was established, which later became ACM's Special Interest Group on IT Education (SIGITE) in 2002. Three later CITC conferences continued to work on the IT Model Curriculum. They initially approved a set of accreditation criteria, which they forwarded to the Accreditation Board for Engineering and Technology (ABET). In April 2005, they published the initial version of an IT model curriculum for public comment. The first formal IT Model Curriculum was published in October 2005 (SIGITE Curriculum Committee, 2005). The IT Model Curriculum was unique from other computing disciplines because it defined its accreditation criteria before its model curriculum.

5.2 Information Assurance and Security (IAS) within the IT Curriculum

One of the unique outcomes of the development of the IT Model Curriculum is dealing with topics considered essential, but do not seem to fit any specific knowledge unit. The SIGITE Curriculum Committee developed 'pervasive themes. Pervasive themes "*are best addressed multiple times, beginning in the IT fundamentals class and woven like threads throughout the tapestry of the IT curriculum*" (2005). Ekstrom et al. (2006) defined pervasive themes as *"A set of 'big ideas' that reside at the heart of the discipline and that cannot be covered directly, but must somehow be grasped by students as they become proficient in the discipline."* Pervasive themes should be introduced in the first IT course taken by majors that covers the IT Fundamentals (ITF) knowledge area. They, then, should be covered throughout the entire curriculum. All students and faculty should be aware of the themes.

Knowledge Areas (KA) are specific bodies of knowledge within a discipline that are covered within separate courses. When first developing the elements of the IT Model Curriculum, the writers were uncomfortable with the term 'security' as a KA (Dark, Ekstrom, and Lunt, 2006). The Writing Committee found that 'information assurance' covered the broader context. The National Information Assurance Education and Training Partnership (NIETP) defined 'information assurance' as a *"set of measures intended to protect and defend information and information systems by insuring their availability, integrity, authentication, confidentiality, and non-repudiation*" (Dark et al., 2006). The addition of the KA, information assurance and security (IAS), within the IT curriculum is the first place where IAS is defined within any discipline. As a knowledge area, IAS is also being used as part of accreditation.

Within the IT Model Curriculum, 'information assurance and security,' is included in three separate areas: (1) The IT Fundamentals Knowledge Area (KA) for the freshmen; (2) As a 'pervasive theme" throughout all courses within the curriculum; and (3) As a separate KA for seniors integrating all concepts learned earlier as a core competency.

Although IAS is a significant part of the IT Model Curriculum, individual institutions have flexibility in how they implement the standards. One study identified an evident 'information security gap,' within undergraduate IT programs in South Africa (Futcher, Schroder, and von Solms, 2010). Security appeared to be better represented and more mature within postgraduate programs. In those few programs where information security was included, it was on an ad hoc basis with only a few information security aspects covered. Within today's world, individuals need to deal with rapidly changing technologies and with large amounts of information. As a result, students will need to have competencies beyond those technical or narrowly defined skills. Other researchers found that as systems technology is rapidly improving within business, the systems are also

becoming less secure. Garfinkel (2012) concluded that the security issue is not being addressed by IT professionals nor within individual academic institution's IT curriculum.

More recently, researchers conducted interviews with security industry executives to determine what should be included in an information systems security track at the undergraduate level (Sharma et al., 2013). This study also found that IS graduate programs more often included a specialized security track. This study recognized that IT students *"would have a good chance of securing employment provided they can demonstrate knowledge of key concepts in the security area"* (Sharma, et al., 2013).

Futcher (2010) recommends that students should study information security from three different levels. The first is the 'social perspective,' using social networks such as Facebook, etc., to communicate, collaborate, and interact with each other. Social risks include online predators, personal data thieves, and viruses. The second is from an 'economic perspective,' where information security losses cost billions of dollars annually. As a result, higher education needs to prepare future professionals to 'demonstrate an understanding of the underlying principles of information security (ISec) and their roles and responsibilities (Futcher, et al., 2010). The third perspective is the 'Intellectual and professional challenge.' Information security should be viewed as a distinct value in any enterprise culture that informs and influences employee behavior.

Information assurance and security (IAS) topics are a challenge within many IT programs. Earlier, this paper described the emerging threats from smartphones and tablets for both business and personal use. Clearly developing mobile device security recommendations is an immediate need for business. The remainder of this paper discusses the mobile device technology security 'education needs.'

5.3 Updating the IT Curriculum through the Introduction of Emerging Technology Topics

The need addressed by IT security professionals for IAS to be included in the IT curriculum is not unique. Information Technology is a field with rapidly emerging technologies. IT academic faculty and researchers are continually promoting the introduction of newer (disruptive) technologies into the IT curriculum. Examples include making the case for mainframe education (Murphy et al., 2010), integrating health IS into database courses (Anderson, Zhang, and McMaster, 2011), introducing cloud computing into the curricula (Chen et al., 2012), or integrating ERP/SAP into the IS curricula (Wang, 2011). Mobile computing education is an especially critical need including the need for mobile application development (Babb and Abdullat, 2012) and integrating location-based privacy issues (Lawler, Molluzzo, and Vandepeutte, 2008). This paper continues this trend to evolve the IT curriculum. The next section provides a set of mobile device security education recommendations. These recommendations are then mapped to the IT Model Curriculum / ABET IT Knowledge Areas.

6. MOBILE DEVICE SECURITY (MDS) EDUCATION RECOMMENDATIONS

Mobility business and emerging mobile devices pose new problems for IT professionals. As mentioned earlier, surveys show that IT professionals understand these technologies present a threat, but they do not know how to minimize the threat. Employees also do not understand the threats from mobile devices, including BYOD and corporate issued devices. One solution is education. Everyone needs to be educated on mobile device security and providing college students in information technology programs with a comprehensive education is a good start.

We described the mobile device security issues earlier in this paper. Students in information technology programs should know basic personal mobile device security as well as how to protect organizations from mobile device security threats. The IT Model Curriculum and ABET accreditation standards provide a good platform to integrate mobile device security topics into the IT curriculum. Just as IT educators recognized that security topics alone were not enough and recommended that information assurance and security (IAS) be included as both a 'Knowledge Area' and a pervasive theme, we recommend that mobile device security topics be included starting with the introduction fundamentals course through the final capstone course. The following discusses our IT education recommendations for integrating mobile device security into the IT curriculum.

6.1 Mobile Device Security Awareness

All college students should have the opportunity to learn about mobile device security and all information technology students should be required to have such knowledge. Sample topics include educating students on differences in the mobile operating systems, app markets, malware, jailbreaking, rooting, anti-virus, firewalls, passcodes, data privacy and security, and app permissions.

6.2 Mobile Device Secure Application Development

IT students need to understand the importance of secure software app development, particularly techniques to maximize app integrity and minimize the threat of reverse engineering. Sample topics include standardized libraries, cross-platform toolkits, vulnerability testing, automated code analysis, quality assurance, secure communication, secure data, and secure storage.

6.3 Mobile Device Security Policy

IT students need to understand how to create a mobile device security policy concerning both corporate-issued devices and personal devices used at work (BYOD). Sample topics include policy organizational integration, development, distribution, comprehension, compliance, and enforcement.

6.4 Mobile Device Security Awareness Training Development

IT students need to understand how to create a security and awareness program within an organization to educate all employees about mobile device security. Sample topics include training techniques, developing curricula, scope, goals, objectives, motivation, delivery, and maintenance.

6.5 Mobile Device Risk Assessment and Management
IT students should be able to access and manage mobile device risk within an organization. Sample topics include threats, assets, likelihood and consequences, documentation, avoidance, transference, mitigation, acceptance, feasibility, cost-benefit analysis, and MDM.

7. INTEGRATING MOBILE DEVICE SECURITY INTO THE IT CURRICULUM

Successful IT programs must work to identify the necessary balance between technical, interpersonal, and management skills for workplace settings. This past year, the IT faculty at the University of South Carolina began a self-assessment of our current undergraduate IT curriculum to meet three objectives: (1) Keep the IT curriculum relevant to business needs; (2) Identify any critical topics that should be added within the curriculum; and (3) Insure the IT curriculum meets ABET accreditation requirements.

We reviewed our IT curriculum and compared it to the ABET requirements. IT students start with business foundation courses including computer applications, programming, business communication, business law, accounting, management, and human resources. As a result of the curriculum review, the faculty is currently developing a new course to increase the information assurance and security emphasis, which also includes the above mobile device security (MDS) recommendations. The following table maps these MDS recommendations to the ABET Knowledge Area (KA) requirements.

Table 1 shows how we mapped MDS recommendations to the IT Model Curriculum/ABET KAs. The first column lists the ABET KAs. Since we consider MDS recommendations to be a "pervasive theme,' we mapped all five MDS recommendations to the first ABET KA, Information Technology Fundamentals (ITF). Since we do not have the space for a detailed discussion of the specific topics within each MDF, we show the general comments for each MDS in the comments column. We used the same technique for each MDF mapped to specific KAs.

	IT Model Curriculum Topics Knowledge Areas	Mobile Device Security (MDS) Education Recommendation (Recs)	Comments
1	*Information Technology Fundamentals (ITF)* ITF1. Pervasive Themes in IT ITF2. Organizational Issues ITF3. History of IT ITF4. IT and Its Related and Informing Disciplines ITF5. Application Domains ITF6. Application of Math and Statistics to IT	(1) MDS Awareness (2) MDS Secure Application Development (3) MDS Policy (4) MDS Awareness Training Development (5) MDS Risk Assessment and Management	• MDS recommendations should be considered pervasive themes (All MDS Recs/ ITF1-5). • All recommendations should be introduced in the Fundamentals (ITF) Introduction course (All MDS Recs/ ITF1-5).
3	Information Assurance and Security (IAS) IAS1. Fundamental Aspects IAS2. Security, Mechanisms (Countermeasures) IAS3. Operational Issues IAS4. Policy IAS5. Attacks IAS6. Security Domains IAS7. Forensics IAS8. Information States IAS9. Security Services IAS10. Threat Analysis Model IAS11. Vulnerabilities	(1) MDS Awareness (3) MDS Policy	• All college students and IT students should be required to know about MDS (MDS Rec 1/ IAS 1, 5, 11). • IT students need to understand how to create a mobile device security policy concerning both corporate-issued devices and BYOD (MDS Rec 3/ IAS4).
7	*Programming Fundamentals (PF)* PF1. Fundamental Data Structures PF2. Fundamental Programming Constructs PF3. Object-Oriented Programming PF4. Algorithms and Problem-solving PF5. Event-Driven Programming PF6. Recursion	(2) MDS Secure Application Development	• IT students need to understand the importance of secure software app development, particularly techniques to maximize app integrity and minimize the threat of reverse engineering (MDS Rec2/ PF1-6).
8	*Platform Technologies (PT)* PT1. Operating Systems PT2. Architecture and Organization PT3. Computer Infrastructure PT4. Enterprise Deployment Software PT5. Firmware PT6. Hardware	(2) MDS Secure Application Development	• IT students need to understand the importance of secure software app development, particularly techniques to maximize app integrity and minimize the threat of reverse engineering (MDS Rec2/ PT1-6).

9	*Systems Administration & Maintenance (SA)* SA1. Operating Systems SA2. Applications SA3. Administrative Activities SA4. Administrative Domains	(3) MDS Policy (5) MDS Risk Assessment & Management	• IT students need to understand how to create a mobile device security policy concerning both corporate-issued devices and BYOD (MDS Rec 3/ SA3). • IT students should be able to assess and manage mobile device risk within an organization (MDS Rec 5/ SA1-4).
10	*Systems Integration & Architecture (SIA)* SIA1. Requirements SIA2. Acquisitions / Sourcing SIA3. Integration SIA4. Project Management SIA5. Testing and OA SIA6. Organizational Context SIA7. Architecture	(2) MDS Secure Application Development	• IT students need to understand the importance of secure software app development, particularly techniques to maximize app integrity and minimize the threat of reverse engineering (MDS Rec 2 / SIA1-7).
11	*Social and Professional Issues (SP)* SP1. Technical Writing for IT SP2. History of Computing SP3. Social Context of Computing SP4. Teamwork Concepts and Issues SP5. Intellectual Properties SP6. Legal Issues in Computing SP7. Organizational Context SP8. Professional and Ethical Issues and Responsibilities	(1) MDS Awareness (4) MDS Awareness Training Development (5) MDS Risk Assessment and Management	• All college students and IT students should be required to know about MDS (MDS Rec 1/ SP 5, 6, 8). • IT students need to understand how to create a security and awareness program within an organization to educate all employees about MDS (MDS Rec 4/ SP 2, 3, 4, 7). • IT students should be able to assess and manage mobile device risk within an organization (MDS Rec 5/ SP 5-8).

Table 1: Mobile Device Security Education Recommendations Mapped to ABET Knowledge Areas (Adapted from Lunt and Ekstrom, 2008)

8. DISCUSSION

The need to attract, develop, and retain information technology (IT) professionals has been a top ten CIO IT management concern since the 1990 annual surveys conducted by SIM and academic researchers (Luftman, Kempaiah, and Rigoni, 2009). In the 2008 survey, three of the top ten issues related to IT resources were – Building skills in IT (2nd); Attracting new IT professionals (4th); and Retaining IT professionals (8th). Although not currently on the top ten list, attracting IT professionals is a continuing and significant challenge for most large enterprises. As 'baby boomer' IT professionals start retiring, experts predict that there will be a severe shortage of entry-level IT professionals. Undergraduate information technology (IT) programs have evolved over the last ten years to specifically prepare students for careers in the application and management of information technology. CIOs desire that students graduate with adequate technical skills, an understanding of the business and project environment, and the ability to integrate IT into the business. They also expect, sometimes unrealistically, that the new graduates should be productive on their first day of work and to have a clear understanding of businesses issues as well (Gorka, Miller, and Howe, 2007). As a result, undergraduate-level IT programs include courses to (1) insure that students graduate with necessary knowledge, skills, and attitudes (KSAs), including ethical and moral values, (2) demonstrate that students can integrate their KSAs into real projects in real complex organizational settings, and (3) insure that students understand organizational needs (Keane and Patten, 2010).

8.1 Introducing New Topics into the IT Curriculum

Emerging technologies and new, innovative uses of information technologies require that IT educators continuously improve and adapt the IT curriculum to meet changing business needs. A Model Curriculum, once approved, is not a static document. Ekstrom and Lunt (2010) describe how the relationships between computing and society continue to change as well as the relationships among the computing disciplines. Information Technology as a computing discipline continues to evolve since many aspects of society rely on IT. Accrediting bodies are also changing the assessment models used to evaluate educational programs and institutions. For example, a Systems Engineering Body of Knowledge (BOK) and the addition of Project Management using Project Management International (PMI)'s Project Management Body of Knowledge (PMBOK) principles have been added to the IT Model Curriculum since 2008 (Ekstrom and Lunt, 2010).

Generally, IT educators first study the business problems when considering changes to their curriculum. They conduct surveys with alumni, industry IT executives, and the programs' own industry advisory boards. Then, they

experiment with specific topics and techniques to develop the best method to introduce various emerging topics into their curriculum. Futcher et al., (2010) described three different approaches for adding higher education instruction in information assurance and security. The first approach is to add a single course, which provides more breadth, but less depth. The second is to add a track or a sequence of courses in information assurance and security, which requires many resources. The third approach is to develop a thread, which is a compromise, bridging the gap between a single course and a track. In this approach, information assurance and security is considered a unifying theme across the core curricula. An example of this third approach is the IT Model Curriculum where Information Assurance and Security (IAS) is one of eight separate 'pervasive themes' (Dark et al., 2006). This approach insures that individual topics should be covered throughout the entire IT curriculum, because they cut across all knowledge areas.

Sharma et al., (2013) proposed adding an undergraduate information systems security track to the 2010 Model IS Curriculum. They also identified three approaches including integration, a single course, or a specialized program. They conducted semi-structured interviews with IS security executives to determine current trends and needs, thus also identifying current curriculum challenges. First, the IS security field is very broad and it is difficult to narrow-in on the critical topics in any approach except by having a track. Another difficulty is finding qualified faculty who have critical experiences in the field. Finally, faculty must have very strong network and telecommunications backgrounds.

Integrating emerging technologies throughout the curriculum is considered a more comprehensive approach that actually takes fewer resources because the new topics are generally added to existing courses. Chen et al., (2012) took this approach and mapped cloud technologies to seven existing courses within the undergraduate information system, computer science, and general sciences programs at one major university in Australia. They first identified major cloud components such as 'hosting Websites on cloud' or 'Matlab parallel computing on cloud.' They mapped these components to the technologies and cloud services providers. Then, they mapped the cloud components to course components such as 'data warehousing' or 'visual studio Web services,' which are included in specific courses. This study illustrated how to map an emerging technology into different courses in three separate disciplines within the university.

Other research articles provide very specific details for developing and introducing a single course into the IT Curriculum. Mobile computing is a rapidly growing technology that includes issues with location-based privacy. Lawler, et al., (2008) provided a detailed framework for identifying the critical aspects necessary to consider location-based privacy issues. They provided course modules with details concerning architecture of mobile computing, design and development of mobile computing applications, and privacy constructs including citizens, consumers, ethics, government entities, methodological, and technological. They detailed security topics as well as future trends. Their paper included reference research sites as well. Another specific new course suggestion is the work by Babb and Abdullat (2012) where they re-conceptualized traditional systems development methods to be responsive to changes requiring more agile approaches and to meet mobile business customer needs. They developed a pilot project to overcome the risk and challenges of designing a mobile applications development course. They experimented with a group of their best undergraduate and graduate IT students with one faculty mentor to develop internal iPhone / iOS apps. This approach allowed the faculty to identify possible concerns about the necessary platform and development knowledge as well as testing and deployment. As a result of their experiment, they outlined specific topics for a future course in mobile applications development.

8.2 Need for Mobile Device Security in IT Curriculum

As the earlier industry security studies point out, IT professionals need to know quite a lot about securing mobile devices. Information assurance and security (IAS) topics are a challenge within many IT programs. Its domains include physical security, operational security, personal security, systems security, and network security. Specific risk actions are avoidance, deterrence, prevention, detection, and recovery. As mentioned earlier under the IAS discussion, its high level security goals should be confidentiality, integrity, authentication, access control, non-repudiation, availability, and privacy. Earlier, this paper described the emerging threats from smartphones and tablets for both business and personal use, which, in many ways, are a subset of the IAS challenges. Clearly developing mobile device security recommendations is an immediate need for business.

This paper contributes to the continued update of the IT curriculum in several ways. It outlines the critical needs for mobile device security practices within business. A series of mobile device security (MDS) recommendations were developed, which also can become the MDS education recommendations. These MDS recommendations were mapped against the IT Model Curriculum/ABET KAs as one example of how the integration of MDS into the IT curriculum could be made. Finally, by educating future IT professionals about MDS issues and the potential solutions, the MDM needs of business may be met. The MDS education goal should be that all IT students develop the ability to protect information by recognizing the major legal, ethical, privacy, and security issues in IT.

9. CONCLUSION

This paper identified business issues for emerging mobile device security (MDS). One way to address this need is by preparing undergraduate IT students by adding MDS into the IT curriculum. It is critical that IT students gain knowledge concerning mobile device security from global security issues, security threats and attacks, and security countermeasures. These IT students would then be better able to address these issues when they become professionals. Mobile device security handled in a single course provides more breadth, but less depth. When treated as pervasive theme, mobile device security issues can be integrated into the entire IT curriculum. Within this paper, a series of mobile device security (MDS) recommendations were developed. These MDS recommendations were mapped

against the IT Model Curriculum / ABET KAs as one example of how MDS could be integrated into the IT curriculum. Because the topics are mapped to the knowledge areas, we believe that other institutions could easily add the mobile device security topics to their IT curricula.

10. REFERENCES

Anderson, N., Zhang, M., and McMaster, K. (2011). Integrating Health Information Systems into a Database Course: A Case Study. *Information Systems Education Journal*, *9*(6), 38-43.

Arxan. (2012). State of Security in the App Economy: 'Mobile Apps Under Attack.' Retrieved 02/09/2013, from http://www.arxan.com/assets/1/7/state-of-security-app-economy.pdf.

Babb, J. S., and Abdullat, A. (2012). The Need for Mobile Application Development in IS Curricula: An Innovation and Disruptive Technologies Perspective. *Information Systems Education Journal*, *10*(1), 61-74.

Chen, L., Liu, Y., Gallagher, M., Pailthorpe, B., Sadiq, S., Shen, H, T., and Li, X. (2012). Introducing Cloud Computing Topics in Curricula. *Journal of Information Systems Education*, *23*(3), 315-324.

Dark, M., Ekstrom, J. J., and Lunt, B. M. (2006). Integration of Information Assurance and Security into Education: A Look at the Model Curriculum and Emerging Practice. *Journal of Information Technology Education*, *5*, 389-403.

Dery, K., and MacCormick, J. (2012). Managing Mobile Technology: The Shift from Mobility to Connectivity. *MIS Quarterly Executive*, *11*(4), 159-173.

Doomun, D.R. (2008). Multi-level Information System Security in Outsourcing Domain. *Business Process Management Journal*, *14*(6), 849-57.

Ekstrom, J. J., Gorka, S., Kamali, R., Lawson, E., Lunt, B., Miller, J., and Reichgelt, H. (2006). The Information Technology Model Curriculum. *Journal of Information Technology Education*, *5*, 343-361.

Ekstrom, J.J., and Lunt, B. M. (2010). Academic IT and Adjacent Disciplines 2010. *Proceedings of the 2010 ACM Conference on Information Technology Education, SIGITE '10*, 1-8.

ESET. (2013), Trends for 2013.

Fahl, S., Harbach, M., Muders, T., Baumgartner, L., Freiseleben, B., and Smith, M. (2012). Why Eve and Mallory Love Android: An Analysis of Android SSL (in) Security. *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, 50-61.

Forrester Consulting. (2012). The Expanding Role of Mobility in the Workplace. *White Paper*, Forrester Research, Inc., Cambridge MA, USA.

Futcher, L., Schroder, C., and von Solms, R. (2010). Information Security Education in South Africa. *Information Management and Computer Security*, *18*(5), 366-74.

Garfinkel, S. (2012). The Cybersecurity Risk. *Communications of the ACM*, *5*(8), 29-32.

Gartner. (2013). Gartner Says Free Apps Will Account for Nearly 90 Percent of Total Mobile App Store Downloads in 2012. Retrieved 02/09/2013, from http://www.gartner.com/newsroom/id/2153215.

Greenberg, A. (2012). Google Gets Serious About Android Security, Now Auto-Scans App Market For Malware. *Forbes*, 2/2/2012. Retrieved 02/11/13, from http://www.forbes.com/sites/andygreenberg/2012/02/02/google-gets-serious-about-android-security-now-auto-scans-app-market-for-malware.

Greenberg, A. (2013). Evasion Is the Most Popular Jailbreak Ever: Nearly Seven Million iOS Devices Hacked in Four Days. *Forbes*, 2/8/2013. Retrieved 02/12/13, from http://www.forbes.com/sites/andygreenberg/2013/02/08/evasi0n-is-the-most-popular-jailbreak-ever-nearly-seven-million-ios-devices-hacked-in-four-days/.

Gorka, S., Miller, J. R., and Howe, B. J. (2007). Developing Realistic Capstone Projects in Conjunction with Industry. *Proceedings of the Annual Conference of the Special Interest Group on Information Technology Education (SIGITE 07)*, October 18-20, Destin FL, USA.

Hoffman, D. (2013). Exposing Your Personal Information – There's an App. *J-Net Community*. Retrieved 02/09/2013, from http://forums.juniper.net/t5/Security-Mobility-Now/Exposing-Your-Personal-Information-There-s-An-App-for-That/ba-p/166058.

Kaspersky. (2013). Kaspersky Security Bulletin 2012: The Overall Statistics for 2012. Retrieved 02/11/2013, from http://www.securelist.com/en/analysis/204792255/Kaspersky_Security_Bulletin_2012_The_overall_statistics_for_2012.

Keane, L. B., and Patten, K. (2010). Information Technology Education: Experiential Learning Benefits. *Communications of Global Information Technology*, *2*, 89-100.

Lawler, J. P., Molluzzo, J. C., and Vandepeutte, P. (2008). An Expanded Study of Integrating Issues of Location-based Privacy with Mobile Computing into General Curriculum of Universities. *Information Systems Education Journal*, *6*(47).

Lawson, E., Lunt, B. M., Reichgelt, H., Ekstrom, J. J., Kamali, R., Miller, J., and Gorka, S. (2005). The Information Technology Model Curriculum. *Proceedings of the ISECON (Information Systems Education Convention*, October 6-9, Columbus OH.

Lookout. (2012). State of Mobile Security 2012. Retrieved 02/11/2013, from https://www.lookout.com/resources/reports/state-of-mobile-security-2012.

Lookout. (2013). 2013 Mobile Threat Predictions. Retrieved 02/11/2013, from https://blog.lookout.com/blog/2012/12/13/2013-mobile-threat-predictions/.

Luftman, J., and Derksen, B. (2012). Key Issues for IT Executives 2012: Doing More with Less. *MIS Quarterly Executive*, *11*(4), December, 207-218.

Luftman, J. N., Kempaiah, R., and Rigoni, E. H. (2009). Key Issues for IT Executives 2008. *MIS Quarterly Executive*, *8*(3), September, 151-159.

Lunt, B.M., and Ekstrom, J. J. (2008). The Model IT Curriculum: A Status Update. *Proceedings of the SIGITE 08 Conference*, Cincinnati OH, 10/16-18/2003.

Mansfield-Devine, S. (2012a). Android Architecture: Attacking the Weak Points. *Network Security*, *2012*(10),

5-12. Retrieved 2/11/2013, from http://dx.doi.org/10.1016/S1353-4858(12)70092-2.
Mansfield-Devine, S. (2012b). Android Malware and Mitigations. *Network Security*, *2012*(11), 12-20. Retrieved 2/11/2013, from http://dx.doi.org/10.1016/S1353-4858(12)70104-6.
Mansfield-Devine, S. (2012c). Paranoid Android: Just How Insecure Is the Most Popular Mobile Platform? *Network Security*, *2012*(9), 5-10. Retrieved 2/11/2013, from http://dx.doi.org/10.1016/S1353-4858(12)70081-8.
Mansfield-Devine, S. (2013). Security Review: The Past Year. *Computer Fraud & Security*, *2013*(1), 5-11. Retrieved 2/11/2013, from http://dx.doi.org/10.1016/S1361-3723(13)70006-X.
McAfee. (2012). Mobile Devices Increasingly Vulnerable to Malware. Retrieved 02/09/2013, from http://www.mcafee.com/fr/solutions/cloud-security/news/20121001-01.aspx.
Murphy, M. C., Sharma, A., Seay, C., and McClelland, M. K. (2010). Alive and Kicking: Making the Case for Mainframe Education. *Information Systems Education Journal*, *8*(14).
Platform Versions. (2013). Platform Versions. Retrieved 02/05/2013, from http://developer.android.com/about/dashboards/index.html
Raphael, J. R. (2012). Exclusive: Inside Android 4.2's Powerful New Security System. *Computerworld Blogs*. Retrieved 02-08-2013, from http://blogs.computerworld.com/android/21259/android-42-security.
Rubens, P. (2012). Mobile Device Management (MDM) Platform Buying guide. Enterprise Network Planet, 08/16/12. Retrieved 2/13/13, from http://www.enterprisenetworkingplanet.com/netsecur/mobmob-device-management-mdm-buying-guide-1.html.
SANS. (2012). SANS Mobility / BYOD Security Survey. Retrieved 02/11/2013, from https://www.sans.org/reading_room/analysts_program/mobility-sec-survey.pdf.
SIGITE Curriculum Committee. (2005). Computing Curriculum 2005. *IT Volume*. Retrieved from http://www.acm.org/education/curric_vols/IT_October_2005.pdf.
Sharma, A., Murphy, M. C., Rosso. M., and Grant, D. (2013). Developing an Undergraduate Information Systems Security Track. *Information Systems Education Journal*, *11*(4), 10-17.
Statcounter. (2013). Top 8 Mobile Operating Systems in the United States from Jan 2012 to Jan 2013. *StatCounter Global Stats.* Retrieved 02/12/13, from http://gs.statcounter.com/#mobile_os-US-monthly-201201-201301.
Strohmeyer, R. (2011). Why I Get Apps from Amazon, Not Google. *PCWorld*. Retrieved 02/11/13, from http://www.pcworld.com/article/239270/why_i_get_apps_from_amazon_not_google.html.
Tenable-Security. (2012). Mobile Device Vulnerability Management Flagged as Top Concern for Security Professionals in 2012. Retrieved 02/12/13, from http://www.tenable.com/news-events/press-releases/2012-mobile-device-vulnerability-management-flagged-as-top-concern-for-se.
The Joint Task Force for Computing Curricula 2005 (2005). *Computing Curricula 2005: The Overview Report.* Computing Curricula Series, ACM.
Thomson, G. (2012). BYOD: Enabling the Chaos. *Network Security*, 2012(2), 5-8. Retrieved 2/13/2013, from http://dx.doi.org/10.1016/s1353-4858(12)70013-2.
Trend Micro. (2012). Evolved Threats in a 'Post-PC' World. Retrieved 02/11/2013, from http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-evolved-threats-in-a-post-pc-world.pdf.
Unknown. (2012). Latest Android Problems and Fixes. *Network Security*, *2012*(11), 2-5. Retrieved 2/13/2013, from http:// dx.doi.org/10.1016/S1353-4858(12)70098-3.
Wang, M. (2011). Integrating ERP/SAP to Information Systems 2010 Curriculum: Design and Delivery. *Information Systems Education Journal*, *9*(5), 97-104.
ZDNet. (2013). Does Jailbreaking or Rooting Devices and BYOD Mix? *ZDNet.* Retrieved 02/12/13, from http://www.zdnet.com/does-jailbreaking-or-rooting-devices-and-byod-mix-7000011069/.

AUTHOR BIOGRAPHIES

Karen P. Patten is an assistant professor in the Integrated Information Technology Program at the University of South Carolina, Columbia, SC. She earned her Ph.D. from the New Jersey Institute of Technology and her M.S. in Civil Engineering from the University of Minnesota. She teaches IT project management, hospitality and tourism IT, and telecommunications and networking. Her research interests include agile and flexible IT management, small business mobile telecommunications management, and IT curriculum development. She is the author of *Data Networking Made Easy* and co-author of Information Technology for Small Business. She has published articles in *Communications of the Association for Computing Machinery, Communications of the Association for Information Systems, Cutter IT Journal, and the International Journal of Computers, Systems and Signals*. Prior to her academic career, Dr. Patten was a Senior Manager for Emerging Technologies at AT&T Bell Laboratories.

Mark A. Harris is an assistant professor in the Integrated Information Technology program at the University of South Carolina, Columbia, SC. He has a Ph.D. in Information Systems from Virginia Commonwealth University, a MS in E-commerce and a BS in Information Technology from Old Dominion University. His research interests

include security policy management, awareness training, human factors of security, health IT security, and mobile device security. He has authored multiple papers in well-respected refereed information systems journals and conferences. Before academia, Mark was a senior network engineer for a large university, where he oversaw an extensive computer network.